**Gergely Barabás**[*]

# Evolution and Revolution of Supervisory Authority Powers in Hungary with Special Regard to the GDPR

*GDPR is a game changer in European data protection law. It has brought revolutionary changes, the fundamental and complete transformation of the role of supervisory authorities, their proceedings and relationship with the judiciary. GDPR has radically raised privacy-awareness across organisations of any kind and it is a radical breakthrough in data subjects', data controllers' and the courts' beliefs and behaviours with regard to the importance of data protection.*

*Hungarian data protection law has also come a long way, with a number of substantive, procedural and organisational changes. Nevertheless, the tendencies are clearly moving in one direction: due to the brutal growth of the data-based economy and services, the protection of personal data requires strong and effective powers. The development of data protection law in Hungary has already directed the organisational and procedural legal framework to an administrative-type model by establishing a more and more effective toolbox of corrective powers even before the GDPR. As regards the role of administrative justice in this process, the administrative judiciary in Hungary more and more actively claims a decisive role in the interpretation of data protection law. This process is far from over, on the contrary we are at the very beginning. The subject of this paper is to present the changes that have taken place in Hungary over the past 30 years, with special regard to the impact of the unified European data protection regulation. The analysis goes through the significant stages of data protection law and shows how the GDPR has generated developments in the powers of the supervisory authority.*

***Keywords:*** *Data protection, Administrative authority, Supervisory authority, Administrative justice, Judicial review, GDPR, Corrective powers, Data protection administrative procedure at the request of the data subject, Data protection administrative procedure ex officio, Temporary corrective powers.*

[*] Legal Counsel, Head of Department of Legal Counsels, Hungarian National Authority for Data Protection and Freedom of Information.

"*They can keep track of what I phoned and when, why, and to whom.*
*They write in files what I dreamed of, and also, who understands it.*
*And I can't guess when there'll be enough reason to look up the file*
*which violates my rights. […]*
*My leader controls me from within! We are humans, not beasts --*
*we are minds! Our hearts, while we desire, not data in a file.*
*Come, freedom! You give birth to an order for me,*
*educate with nice words, but let it play too,*
*your handsome, serious son!*"

***József Attila[**] / "I can't breathe" / 1935***

## 1. Introduction

The National Authority for Data Protection and Freedom of Information (hereinafter "the Authority" or "the NAIH") in Hungary is responsible for monitoring and promoting the enforcement of two fundamental rights: the right to the protection of personal data and the right to freedom of information (access to data of public interest and data accessible on public interest grounds). The Authority is also authorised to launch a procedure for the supervision of classified information in order to establish whether classification is lawful.

Based on constitutional provision, the Act CXII of 2011 on the right to informational self-determination and on the freedom of information (hereinafter "the Act CXII of 2011"), which entered into force on 1 January 2012, established the Authority and regulated its operation in detail. From an organisational perspective, the NAIH is an autonomous state administration organ; it shall not be instructed in its functions and shall operate independently of other organs and of undue influence. The tasks of the NAIH shall only be determined by an Act of Parliament.

However, regarding the organisational and procedural landscape this has not been always the case.

The first general data protection act (Act LXIII of 1992 on the Protection of Personal Data[1] and Public Access to Data of Public Interest[2]; hereinafter "the Act LXIII of 1992) in Hungary – as one of the cornerstones of the rule of law – entered into force in 1993 after the change of regime.

[**] 1 April 1905 – 3 December 1937 – József Attila was one of the most famous Hungarian poets of the 20th century. Generally, not recognized during his lifetime, József become the best known of the modern Hungarian poets internationally.

[1] Article 2(1): 1. 'personal data' shall mean any data relating to a specific (identified or identifiable) natural person (hereinafter referred to as 'data subject') as well as any conclusion with respect to the data subject which can be inferred from such data. In the course of data processing such data shall be considered to remain personal as long as their relation to the data subject can be restored. An identifiable person is in particular one who can be identified, directly or indirectly, by reference to his name, identification code or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

[2] Article 2(4) 'data of public interest' shall mean any information or knowledge, not falling under the definition of personal data, processed by an organ or person performing a state or local government function or other public function determined by a rule of law, or any information or knowledge pertaining to the activities thereof, recorded in any way or any form, irrespective of the manner it is processed and its independent or collected character.

The Act LXIII of 1992 had the following rules relating to judicial enforcement of data protection rights.

In case of infringement of his rights the data subject may institute court proceedings against the data controller.[3] The burden of proof that the data processing has been in compliance with the pertaining rules of law shall lie with the data controller.[4] The data controller shall be liable for any damage suffered by data subjects as a result of an unlawful processing of their data or as a result of an infringement of the technical requirements of data protection. The data controller shall also be liable for any damage suffered by the data subject resulting from the actions of a technical data processor. The data controller shall be exempted from liability if he proves that the damage was the result of force majeure beyond the sphere of data processing.[5] No compensation shall be paid for the part of damage suffered by the damaged person as a result of his intentional or grossly negligent conduct.[6]

The rules set out in Articles 17-18 provided for the litigation(s) between the data subject and the data controller fell within the jurisdiction of the civil courts.

However, the other pillar of judicial protection was almost completely missing from the Hungarian data protection system for a long time: the judicial review[7]. This was primarily due to the fact that the Data Protection Commissioner which was established by the Act LXIII of 1992[8] did not act as an administrative authority, its powers were '*soft*', that is, the Commissioner did not issue legally binding administrative decisions due to its legal status, and as a result its legal positions as administrative decisions "ruling" on the lawfulness of processing operations could not be brought before the administrative judge. On the other hand, according to the theory of data protection law in Hungary which reflected in the substantive text of the law, processing operations belonging to public administration did not qualify as an administrative activity or act the assessment of the lawfulness of which would have been subject to judicial review. The lawsuit brought before court by the data subject in relation to processing operations of administrative bodies had been considered as civil law litigations.

The result of this overall regulatory concept established by the Act LXIII of 1992 was that the legal interpretation issues related to protection of personal data *almost completely* avoided the administrative courtrooms for about two decades. The "case-law" developed by the Data Protection Commissioner could thus evolve over a long period of time by means of "*soft law*" without either the data subjects or the controllers having been able to challenge the compliance of processing operations with the law before administrative courts.

The Fundamental Law of Hungary[9] and the Act CXII of 2011 by establishing expressly the Authority as an administrative authority[10], transferred the protection of personal data to the

[3] Article 17(1).
[4] Article 17(2).
[5] Article 18(1).
[6] Article 18(2).
[7] Judicial review is a type of court proceeding in which a judge reviews the lawfulness of a decision or action made by a public body.
[8] Article 23(1) In order to safeguard the constitutional right to the protection of personal data and to public access to data of public interest, Parliament shall elect a Data Protection Commissioner from among Hungarian citizens with a university degree, a clean criminal record and an outstanding academic knowledge or at least 10 years of professional practice, who have significant experience either in conducting or supervising proceedings involving data protection or in the scientific theory thereof.
[9] The Fundamental Law of Hungary (25 April 2011).
[10] Article VI of the Fundamental Law of Hungary (1) Everyone shall have the right to have his or her private and family life, home, communications and good reputation respected. Exercising the right to freedom of expression

competence of a supervisory public authority and embedded it more strongly into the public sphere[11]. The judicial review of the decisions of public authorities is a constitutional requirement in all States based on the rule of law.

The establishment of the Authority and the enforceability of the protection of personal data through public powers have created a fundamentally new situation for the administrative judiciary, as well. This is the case even if it is factually true that the Act LXIII of 1992 had already given in 2004 the Data Protection Commissioner a toolbox of public powers[12] which, in terms of its legal status, would probably have strengthened its role as a public authority.

## 2. Enforcement of the Act LXIII of 1992 (1993-2012)

### 2.1. The Beginnings

As I have already noted, during this period data protection law issues *almost completely* avoided the administrative judiciary courtrooms.

It cannot be stated that the provisions of the Act LXIII of 1992 were completely unknown to administrative judges. The reference to the rules of this Act was indeed part of the administrative litigations in other groups of cases, although, as mentioned above, the reference to data protection infringements appeared rather as an auxiliary feature in lawsuits against administrative decisions – for example in tax and competition cases. The administrative judges dealing with tax, competition or other administrative cases did not consider it to be evident that, in the case brought before them, whether directly or indirectly, it was for them to interpret the rules of the Act LXIII of 1992 and to rule on their correct interpretation in order to assess the legality of a different type of administrative act.

### 2.2. Relationship Between Data Protection and Other Fields of Law

and assembly shall not impair the private and family life and home of others. (2) The State shall provide legal protection for the tranquillity of homes. (3) Everyone shall have the right to the protection of his or her personal data, as well as to access and disseminate data of public interest. (4) The enforcement of the right to personal data protection and the right of access to data of public interest shall be monitored by an independent authority established by a cardinal Act.

[11] Section 38 (1) -(2) of the Act CXII Section (1) The Authority shall be an autonomous state administration organ. (2) The Authority shall be responsible for monitoring and promoting the implementation of the right to personal data protection and the right of access to data of public interest and data accessible on public interest grounds, as well as for promoting the free movement of personal data within the European Union.

[12] Article 25(4) -(5) of the Act LXIII of 1992 (4) If the data controller or technical data processor fails to discontinue the unlawful processing (technical processing) of personal data, the Data Protection Commissioner may order in a decision the blocking, deletion or destruction of unlawfully processed data, prohibit the unlawful processing or technical processing of data, and suspend the transfer of data to foreign countries. The decision may not be remedied in administrative way. (5) The data controller, the technical data processor or the data subject may request judicial review from the court against the decision of the Data Protection Commissioner pursuant to paragraph (4) – within 30 days after its receipt – on the grounds of infringement. The Court shall proceed according to the regulations on lawsuits against public administration of the Civil Procedure Act. Until a final court decision, the data concerned may not be deleted or destroyed; the processing of data, however, shall be suspended and the data shall be blocked.

An illustrative example of the above-mentioned practice is the tax case in which the administrative court did not examine the lawfulness of the tax authority's processing operation in spite of the applicant's express claim, simply on the basis of lack of competence. The applicant complained that, on the basis of a letter of assignment, the tax authority was authorised by law only to collect data relating to the undertaking during the course of the tax investigation, but the tax authority went beyond that scope and made extra-enquiries among the applicant's private bank accounts, private vehicles and real estate. According to the applicant, the tax authority infringed the rules of the Act LXIII of 1992 and he objected as a data subject to the processing of his personal data by the tax authority. He also stated that he did not intend to lodge a separate data protection procedure against the tax authority.

The answer of the administrative court *was the following: "[p]ursuant to Section 16/A[13], the administrative court has no jurisdiction in relation to the processing of personal data. If the data subject, in this case the applicant, objects to the processing of his or her personal data, the controller – the tax authority – has to decide on this. If the data subject does not agree with the decision, he/she may apply to a civil court of general jurisdiction. In the absence of its own jurisdiction, the administrative court could not deal with the data protection objection on the merits in the tax case.'[14]* In this judicial argument, the strange is not what it records, but what it does not. It simply failed to argue why the court did not consider it possible to review the tax authority's decision on that basis. The action complained not only about the right to object, but also a breach of more general data protection provisions. This judicial argument sought to separate the role of the administrative authority as an authority from that of a controller.

The above-mentioned administrative judicial attitude is even more clearly illustrated by a judgement in which the Hungarian Supreme Court did not deal with the aspect of data protection law and its impact on the tax matter. It argues that *"[t]he Civil Code and the Act LXIII of 1992 to which the applicant made reference, do not contain any rules for resolving the tax dispute, and the defendant did not base its decision on non-compliance with the rules laid down by those laws, but on the provisions of financial law governing the resolution of financial disputes."*[15]

The reason for not carrying out the examination of the Act LXIII of 1992 in administrative matters was also explained in an abstract way in competition cases, although there was a judgment which did not entirely exclude the interpretation of this Act while assessing the legality of administrative decisions. In a competition law case the appellant stated that the documentation in the administrative proceedings by the competition authority was carried out in breach of the provisions of the Act LXIII of 1992. The administrative court held that *"[a]ccording to Article 1(1) of the Act, its purpose is to guarantee the right of everyone to exercise control over his or her personal data and to have access to data of public interest, except as otherwise provided by a rule of law under this Act. The applicant did not prove in an identifiable manner which natural person was concerned during the defendant's*

[13] Article 16/A (1) (Right to object) The data subject may object to the processing of his data if a) the processing (transfer) of personal data is necessary solely for enforcing a right or legitimate interest of the data controller or data recipient, except if the data processing has been ordered by an Act; b) personal data are used or transferred for the purposes of direct marketing, public opinion polling or scientific research; or c) the exercise of the right to object is otherwise made possible by an Act.

[14] Vas County Court of Hungary 1.K.20.018/2009/33.

[15] Supreme Court of Justice of Hungary Kfv.V.35.180/2009/5.

*administrative proceedings or which rules of the processing of personal data were violated. Thus, the court was unable to establish an infringement of data protection law.*"[16]

In another competition law case, the Supreme Court essentially held that *"[r]egarding the defendant's proceedings, the applicant erroneously referred to the infringement of the Act LXIII of 1992 in the context of the Article 65(4) of the Act LVII of 1996[17]. Data protection rules apply in individual administrative procedures to the extent that the data protection context is regulated by the respective procedural law. In general, on grounds of data protection law, the administrative procedure regulated by law shall not be called into question, as appropriate processing of personal data in these cases is guaranteed by law. From the point of view of data protection, the administrative procedure may be unlawful, including the decision of the authority, if the rules governing the administrative procedure authorize the examination of such aspects. In the absence of this, processing of personal data may be violated in accordance with the procedure set out in the Act LXIII of 199., however, this constitutes an independent data protection procedure, which must be distinguished from the procedure at issue, that is, competition supervision proceedings. The court of first instance rightly pointed out that the legality of the defendant's decision can and shall be assessed in the administrative proceedings on the basis of the Act LVII of 1996, and the administrative action (investigative measure) could not be subject to judicial review under the Act LXIII of 1992*.'[18]

Administrative courts essentially had not dealt with data protection legal issues for about 20 years.

However, this was not due to the fact that the applicants' actions did not attempt to raise issues of data protection law through the reference of the Act LXIII of 1992.

In most of the cases by using this tool they aimed at claiming and proving the unlawfulness of obtaining evidence by administrative authorities, in order to establish errors in the clarification of the facts of the administrative decisions by excluding unlawfully (in breach of data protection rules) obtained evidence.

But we cannot state that the reference to the general data protection act played only such a role. The arguments which sought to demonstrate that public authorities are obliged

[16] Budapest Court of Hungary K.33.024/2004/46.

[17] Article 65(1) -(6) of the Act LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices (Competition Act) (1) On the summons of the case handler or the competition council proceeding in the case, data recorded in a computing system or on an electronic data storage device (hereinafter collectively: data storage) shall be made available by the possessor of such data storage in a format enabling reading and copying. (2) The case handler and the competition council proceeding in the case shall be entitled to make copies of documents and data stored on a data storage. The case handler shall be entitled to make a forensic copy of the data storage and to inspect its contents using that forensic copy if it is likely to contain data in connection with the conduct under investigation that cannot be retrieved in course of the proper use of the computer. (3) In the process of making an electronic copy of the data stored on the data storage the data shall be recorded in a way that prevents the subsequent manipulation of the data or — if this is not possible due to the type of the data storage — the data shall be recorded using a technology that ensures that it is possible to control the unchanged nature of the data at a later stage. (4) Property may be taken into custody by the case handler by depositing the property into a container suitable for its safeguarding or into a separate room, either of which shall then be locked and sealed. (5) If the property is not available on site, the case handler may take it into custody by obliging the holder of the property to make it available to the Hungarian Competition Authority in an unchanged format, at a specified location and time. (6) Otherwise, custody and seizure shall be subject mutatis mutandis to the provisions of the GRAP Act, with the proviso that with regard to privileged information exemption from confidentiality shall be deemed to have been granted to the holder of the property, with the exception of classified information.

[18] Supreme Court of Justice of Hungary Kfv.37.923/2010/5.

to fulfil their obligations as controllers in the performance of their official functions emerged very quickly and had an impact on their actions. It is apparent, however, that the published case-law lacked a theoretical clarification of data protection law issues and, if it was possible, it emphasized that the lawfulness of an administrative act could be judged solely on the basis of the sectoral administrative rules applicable to it.

### 2.3. The Evolving Role of Data Protection Authority – Section 25(3)-(4) of the Act LXIII of 1992

According to the original Sections 24-25 of the Act LXIII of 1992 the Data Protection Commissioner a) shall supervise compliance with this Act and other rules of law on data processing b) shall investigate notices lodged with him; c) shall ensure the maintenance of the data protection register.[19]

Under Article 25(1) -(3) of this Act the Data Protection Commissioner shall monitor the conditions of the protection of personal data and of the realisation of public access to data of public interest and data public on grounds of public interest. It shall make proposals for the adoption or amendment of legislation on data processing or on public access to data of public interest and data public on grounds of public interest, and give an opinion on such draft legislation. It may initiate a narrowing or broadening of data categories classified as state or service secrets. Upon observing any unlawful processing of data, the Data Protection Commissioner shall call on the data controller to discontinue the data processing. The data controller shall take the necessary measures without delay and inform in writing the Data Protection Commissioner thereof within 30 days. The Data Protection Commissioner may inform the public of the launching of his investigation, of the fact of the unlawful processing (technical processing) of data, of the person of the data controller (technical data processor) and of the range of processed data.[20]

However, on the 1st January 2004, there was a significant[21] change in the Data Protection Commissioner's supervisory "powers". The legislation gave actual administrative-type supervisory corrective powers to the Commissioner. The Act stated that if the data controller or technical data processor fails to discontinue the unlawful processing (technical processing) of personal data, the Data Protection Commissioner may order in a decision the blocking, deletion or destruction of unlawfully processed data, prohibit the unlawful processing or technical processing of data, and suspend the transfer of data to foreign countries. The decision may not be remedied in administrative way. The data controller, the technical data processor or the data subject may request judicial review from the court against the decision of the Data Protection Commissioner pursuant to paragraph (4) – within 30 days after its receipt – on the grounds of infringement. The Court shall proceed according

[19] Article 24.
[20] Article 25(1) - (3).
[21] See the report of 2005 of the Data Protection Commissioner, 45-46; "*The biggest change in the powers of the Data Protection Commissioner was undoubtedly to order the blocking, erasure or destruction of data processed unlawfully after 1 January 2004, or to prohibit unauthorised processing and to suspend the transfer of data abroad. The controller or processor concerned may turn to a court against the decision of the Commissioner, pending the decision of the court, the data processing shall be suspended and the data shall be blocked. However, the law leaves many important questions unanswered. One of these is what happens if the controller does not terminate the unlawful processing and does not go to court: in addition to 'ordering', the Commissioner does not have any authority to impose a fine or order enforcement*.

to the regulations on lawsuits against public administration of the Civil Procedure Act. Until a final court decision the data concerned may not be deleted or destroyed; the processing of data, however, shall be suspended and the data shall be blocked.[22]

The result of these rules was that the Data Protection Commissioner subsequently participated as defendant to administrative lawsuits brought before the administrative judiciary, in other words, the findings and interpretation of the data protection law set out by the Data Protection Commissioner were subsequently *subject to judicial review*.

The new legislation created new challenges for both the Data Protection Commissioner and the administrative judicial practice. In its changed role, the Commissioner had to draft, edit its "*administrative" decisions*" and conduct its proceedings in accordance with the procedural requirements imposed on administrative decisions and proceedings. Meanwhile administrative law judges had to study the previously unexamined and unexperienced depths of data protection law.

Thus, through the Data Protection Commissioner's decisions, not only the processing of personal data of public bodies could be subject to judicial review, but, as the Commissioner was competent to monitor the processing of all public and private bodies, all controllers and processing operations could, in principle, be subject to the control of the administrative judiciary.

The conditional means, however, that the establishment of the above-mentioned corrective powers of the Commissioner did not result in an "*explosion*" of the number of actions against its decisions. In 2004, a total of 2[23] actions were brought before the administrative court[24].

## 3. Entry into Force of the Fundamental Law and the Act CXII of 2011 (1st January 2012 – 25th May 2018)

### 3.1. Introduction of the Ex Officio Data Protection (Supervisory-Type) Administrative Procedure

This period was about the development of the role of the supervisory authority and the extension of the investigative and corrective supervisory powers. It was also another significant step towards a coherent and more detailed data protection administrative judicial practice.

Article VI (2) -(3) of the Fundamental Law on the one hand maintained the Hungarian data protection legal traditions by enshrining the fundamental right to the protection of personal data at the level of the Fundamental Law and on the other hand while triggering a number of procedural and competence consequences it entrusted the monitoring of the exercise of the right to protection of personal data to an '*independent authority*' which was the NAIH.

Section 38(1) established the Authority as an autonomous state administration organ. The Section 38(3) listed the *inter alia* the following tasks of the Authority: the Authority especially a) shall conduct *inquiries* upon notification and ex officio; b) shall conduct

[22] Article 25(4) - (5).
[23] See the Data Protection Commissioner's 2005 report, 35-46.
[24] See the Data Protection Commissioner's 2008 report, 134-135.

*administrative proceedings* for data protection *ex officio*; c) shall conduct administrative proceedings for the supervision of classified information *ex officio*; d) may bring proceedings before the court in connection with any infringement concerning data of public interest and data accessible on public interest grounds; e) may intervene in actions brought by others. Therefore, the Act CXII of 2011 did not abandon the Authority's so-called "*data protection inquiry*" procedure, an ombudsman-type soft power, but meantime it established the *ex officio* administrative procedure for data protection resulting in legally binding administrative decisions subject to judicial review. The Act on the general rules of administrative procedure shall be applied to the *ex officio* data protection administrative procedure.

The latter was established hand in hand with a toolbox of supervisory investigative and corrective administrative powers, which combine reparative and repressive tasks in order to strengthen the enforcement of privacy rights. At this time data protection administrative procedure could be initiated only *ex officio*.

Section 61(1) defined the legal consequences of the infringement of data protection provisions. According to this in its decision adopted in the data protection administrative proceeding, the Authority may order the erasure, in a manner specified by the Authority, of unlawfully processed personal data or it may impose a temporary or definitive limitation on processing in another way, establish that the personal data have been unlawfully processed, order the rectification of any personal data that are inaccurate, order the blocking, erasure or destruction of unlawfully processed personal data, prohibit the unlawful processing of personal data or prohibit the transfer or disclosure of personal data to foreign countries order the provision of information to the data subject if the controller unlawfully omitted or refused to do so, and impose a fine.

The Act CXII of 2011 could not have stated more clearly that the data subjects had not yet been given a legal opportunity to lodge the administrative procedure with their complaint(s).

The NAIH has become a real "*administrative authority*" with all the consequences.

The administrative justice system found itself also in a completely new position. On the basis of the rules of the Act CXII of 2011 the Hungarian administrative judicial practice began to build its own concept in the field of substantive and procedural data protection law, for instance the competence and the conditions of the application of the investigative and corrective powers of the Authority.

### 3.2. Questions About the Competence of the Authority

On the basis of the Act CXII of 2011 the Hungarian administrative judicial practice faced almost immediately with specific issues of data protection law and difficulties in resolving them. These questions led to judgments containing basic guidelines to the applications of data protection norms.

In the history of Hungarian data protection law, the first request for a preliminary ruling was submitted by an administrative court in the Weltimmo case[25]. This request concerned the interpretation of Articles 4(1)(a) and 28(1), (3) and (6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[25] Judgment of 1 October 2015, Weltimmo, C-230/14, EU:C:2015:639.

The request has been made in proceedings between Weltimmo s. r. o., a company which has its registered office in Slovakia, and the Authority concerning a fine imposed by the latter for infringement of Act CXII of 2011 which transposed Directive 95/46 into Hungarian law. Weltimmo run a property dealing website concerning Hungarian properties. For that purpose, it processed the personal data of the advertisers. The advertisements were free of charge for one month but thereafter a fee was payable. Many advertisers sent a request by e-mail for the deletion of both their advertisements and their personal data as from that period. However, Weltimmo did not delete those data and charged the interested parties for the price of its services. As the amounts charged were not paid, Weltimmo forwarded the personal data of the advertisers concerned to debt collection agencies. Those advertisers lodged complaints with the Hungarian data protection authority.

That Authority declared that it was competent, taking the view that the collection of the data concerned constituted processing of data or a technical operation for the processing of data concerning natural persons. Considering that Weltimmo had infringed the Act CXII of 2011, the Authority imposed on that company a fine.

Weltimmo then brought an action before the court which held that the fact that that company did not have a registered office or branch in Hungary was not a valid argument in defence because the processing of data and the supply of data services relating to the Hungarian property concerned had taken place in Hungary. However, that court set aside the decision of the Authority on other grounds, connected with the lack of clarity over some of the facts. Weltimmo appealed on a point of law to the referring court, claiming that there was no need for further clarification of the facts, since, pursuant to Article 4(1)(a) of Directive 95/46, the Hungarian data protection authority in this case was not competent and could not apply Hungarian law in respect of a supplier of services established in another Member State. Weltimmo maintained that, under Article 28(6) of Directive 95/46, that Authority should have asked the Slovak data protection authority to act in its place. The Hungarian data protection authority submitted that Weltimmo had a Hungarian representative in Hungary, namely one of the owners of that company, who represented it in the administrative and judicial proceedings that took place in that Member State. That Authority added that Weltimmo's Internet servers were probably installed in Germany or in Austria, but that the owners of that company lived in Hungary. Lastly, according to that Authority, it followed from Article 28(6) of Directive 95/46 that it was in any event competent to act, regardless of the applicable law.

The Court finally held that Article 4(1)(a) of Directive 95/46/EC must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity — even a minimal one — in the context of which that processing is carried out. In order to ascertain, in circumstances such as those at issue in the main proceedings, whether that is the case, the court may, in particular, take account of the fact (i) that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State's language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to

the processing of the data concerned. By contrast, the issue of the nationality of the persons concerned by such data processing is irrelevant.

As for the supervisory powers of the Authority, the Court stated that where the supervisory authority of a Member State, to which complaints have been submitted in accordance with Article 28(4) of Directive 95/46, reaches the conclusion that the law applicable to the processing of the personal data concerned is not the law of that Member State, but the law of another Member State, Article 28(1), (3) and (6) of that directive must be interpreted as meaning that that supervisory authority will be able to exercise the effective powers of intervention conferred on it in accordance with Article 28(3) of that directive only within the territory of its own Member State. Accordingly, it cannot impose penalties on the basis of the law of that Member State on the controller with respect to the processing of those data who is not established in that territory, but should, in accordance with Article 28(6) of that directive, request the supervisory authority within the Member State whose law is applicable to act.

### 3.3. Scope of the Authority's Corrective Powers

The Authority thus has become an administrative authority not only in its proceedings, but also in terms of administrative sanctions of data protection infringements. As the fundamental nature of these sanctions adversely affect controllers, the conditions and framework under which the Authority may apply them had already been a key issue in administrative lawsuits initiated under the Act CXII of 2011.

The administrative judicial practice based on this Act sought to widen the use of the Authority's toolbox in accordance with the legislative purpose of the Fundamental Law and the Act. Indeed, one of the reasons for the adoption of the Act and the establishment of the Authority was the following: *"[t]he practice of the Commissioner, demonstrated that the powers and tools of the Commissioner did not provide sufficient margin of appreciation and move to investigate and sanction data protection infringements. The spread of information technology, the changing social habits and the new situation created by globalisation require significantly more effective action by public authorities than the system of ombudsman-type Commissioner established in the mid-90s could provide. An administrative authority is a more appropriate organisational form, so it is necessary to establish an authority capable of facing new challenges. The new circumstances necessitate the establishment of a new regulation and organisation in this area that fits into the concept of the Fundamental Law and meets the expectations of the European Union.'*[26]

The Kúria's (Supreme Court of Hungary) approach was in accordance with the this purpose: according to the Kúria "[*t]he Section 61(1)(a) to (g) determines the nature of the measures that may be applied in the decision of the data protection authority. The corrective toolbox covers, for example, the possibility of establishing unlawful processing of personal data, prohibiting the continuation of processing, blocking the unlawfully processed personal data, ordering the termination of their transfer abroad or imposing fines."*[27]

For example, in the context of an *ex officio* prohibition of processing, the reasoning of the court was that " *[p]rocessing of personal data may violate data protection rules in a number of ways with different behaviours and omissions. It is impossible to list them in detail,*

[26] Preparatory document to the Act XCII of 2011.
[27] Kúria Kfv.III.37.911/2017/8.

*so the Act CXII of 2011 provides in general for the possibility of prohibiting unlawful processing. Those corrective powers of the Authority must be fulfilled by the defendant in the specific case, having regard to the specific features of the case [...].*"[28]

## 4. The GDPR[29] (2018): Interplay Between the EU and Hungarian Law

### 4.1. A Revolutionary Change: Data Protection Administrative Procedure at the Request of the Data Subject

On the 25th May 2018, the GDPR entered into force in the above-mentioned circumstances: an increasingly extensive and deepening administrative judicial practice was about to develop. The GDPR did not send the judicial and administrative practice back to the start line.

However, it is worth pointing out some orientations that might determine the interpretation of the GDPR in the future.

Regulation introduced a "*revolutionary*" innovation in the Hungarian law. Article 77(1) of the GDPR provides that, without prejudice to any other administrative or judicial remedy, each data subject shall have *the right to lodge a complaint with a supervisory authority*, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her infringes this Regulation. In this context, Article 78(1) provides that, without prejudice to any other administrative or non-judicial remedy, every natural or legal person shall have the *right to an effective judicial remedy against a legally binding decision of a supervisory authority* concerning him or her.

The Hungarian legislation – in accordance with Article 41 and 47 of the Charter of Fundamental Rights of the European Union – translated these rules into the Hungarian administrative procedural legislation by opening the possibility of lodging an administrative procedure before the Authority *at the request (complaint) of the data subject*. That is why Section 60(1) of the Act CXII of 2011 provides now that to give effect to the right to personal data protection, the Authority shall bring administrative proceedings for data protection *on the application of the data subject* and may bring administrative proceedings for data protection *ex officio*.

This apparently simple rule has raised a series of questions of interpretation not only in the practice of the Authority but also in the practice of the administrative law courts. Indeed, the general administrative procedure theory makes a clear distinction between administrative procedures initiated at the party's *request* and those initiated *ex officio*. Articles 77 to 78 of the GDPR, apart from requiring a decision by a supervisory authority with legally binding power and effective judicial review, do not contain any further procedural rules governing the specific proceedings under national law, in accordance with the EU law principle of institutional and procedural autonomy of the Member States.

[28] Kúria Kf.VI.37.956/2018/6.

[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) (hereinafter 'the GDPR').

A distinguishing feature of the procedure lodged at the request of the data subject is that in this case the administrative procedure is initiated not on the basis of the professional appreciation of the Authority, but at the will of the data subject. No professional legal help is required in the proceedings before the Authority under the GDPR. However, this leads to the practical consequence that the quality and the content of the requests to carry out the procedure are extremely diverse.

Submitting the application, the data protection administrative procedure is automatically open in accordance with the provisions of the GDPR and national general administrative procedure act. The problem is that while the Authority must draft a sufficiently detailed and justified decision in this type of procedure, as well, the content of the requests often does not allow it to do so, and the Authority often faces incomplete, contradictory and undocumented claims for which even the cooperating controllers find it difficult to provide meaningful answers.

However, this is one of the classic and fundamental questions of the administrative procedure and litigation: the extent to which the administrative authority, in this case the Authority, has an obligation to clarify the facts and to state reasons, and when it reaches the certainty of the decision to establish data protection liability and to impose a serious administrative sanction against an entity as required by the GDPR. It is clearly stated in the case-law that the Authority is not a law-enforcement authority conducting criminal investigation.

The Authority is often confronted with the fact that it can rely only on a small number of evidence, including the data subject's request and the parties' statements made in the course of the procedure, which are evidently contradictory in most cases.

According to the Kúria in principle *"[i]n the proceedings lodged at the request of the data subject, the Authority shall establish the facts to the extent which is necessary for the adoption of the decision and, accordingly, it shall carry out the procedure in order to find the relevant pieces of evidence. However, the Authority is not obliged to seek evidence of the applicant's interest. […]".* It is also established case-law that it is for the applicant to prove the unlawfulness of the Authority's decision in the action before the administrative law court. According to the Curia, it is up to the applicant to prove that the contested decision is vitiated by an infringement of law.

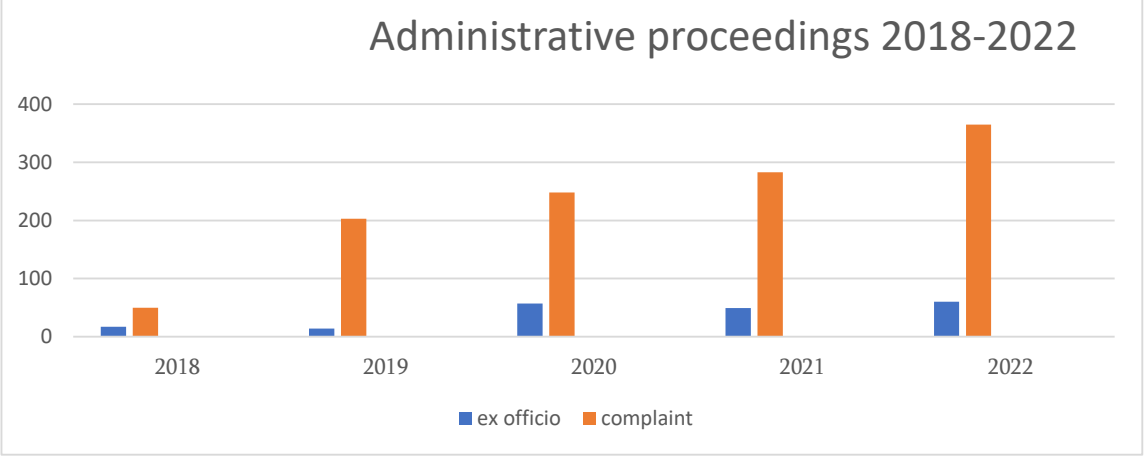
The requests under the GDPR often contain only statements or assumptions, but the data subject is unable to produce any tangible evidence from which any aspect of the specific processing of personal data, the legality or illegality of the latter can be established. It is precisely for this reason that judicial practice has stated, in line with the above, that *"[i]n the absence of processing of personal data actually available, it is not possible to carry out objectively a substantive examination of the request by the Authority."*

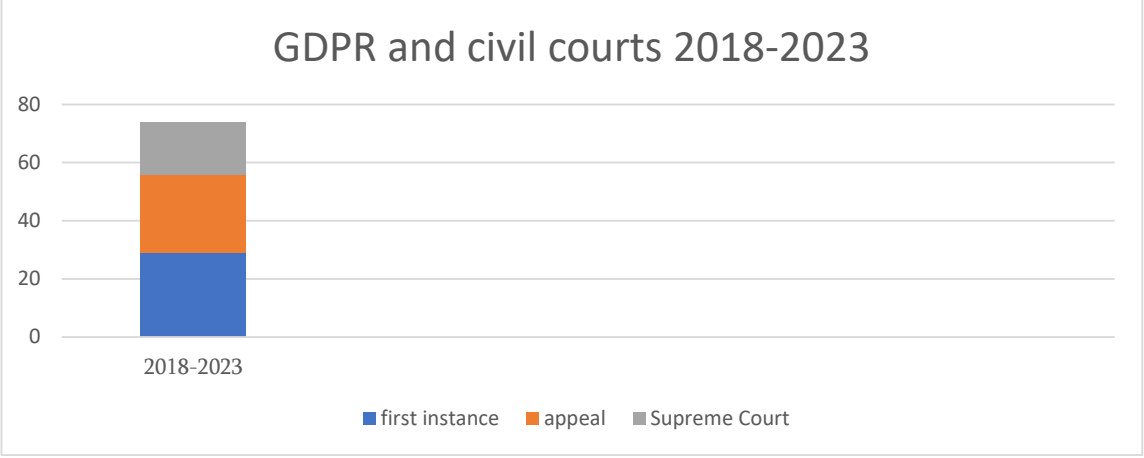
However, before I am going to analyse the most important current issues related to the Authority's corrective powers, let the figures talk about the revolutionary changes introduced in connection with the entry into force of the GDPR. Despite the undoubted procedural difficulties, the GDPR really generated significant changes for data subjects so that they can enforce their data protection rights guaranteed by the GDPR.

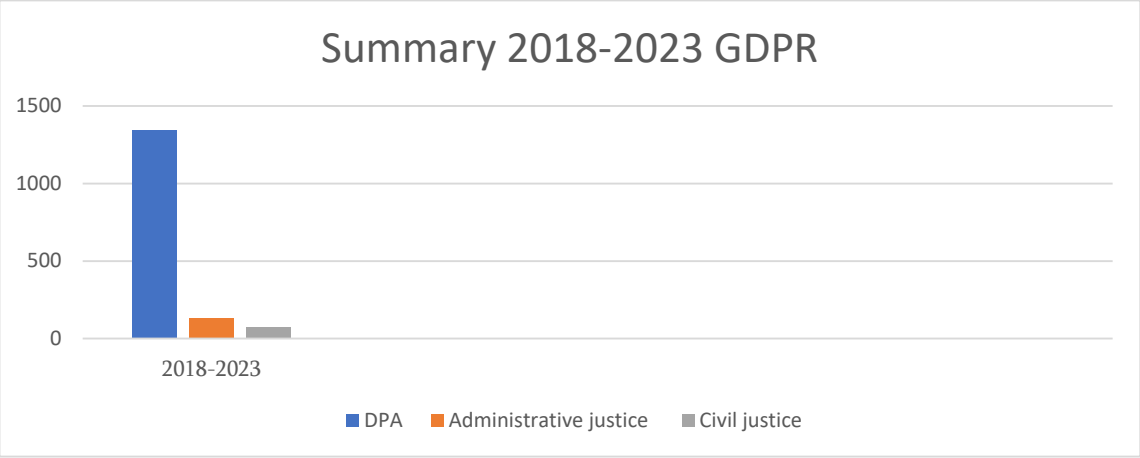
Let us see the statistics before and after the entry into force of the Regulation:

- Number of administrative lawsuits on the basis of former domestic data protection laws 2004-2018 (entry into force of the GDPR): 60;
- Number of administrative lawsuits on the basis of the GDPR 2018-2023: 131 (first instance, appeal and review closed by judgment) [Art. 78 of the GDPR];

- Number of civil lawsuits on the basis of the GDPR 2018-2023: 74 (first instance, appel and review closed by judgment) [Art. 79. of the GDPR];
- Number of references for preliminary rulings 2004-2018 (95/46/EC): 1 (by an administrative court);
- Number of references for prelimimary rulings 2018-2023 (GDPR): 4 (all by administrative courts);
- Number of references for preliminary rulings 2004-2018 (in general): 94;
- Number of references for preliminary rulings 2018-2023 (in general): 27 [15% of the overall Hungarian requests concern data protection issue (!)];
- Number of data protection administrative proceedings *at the request of data subjects* 2004-2018: 0 (as only *ex officio* administrative proceedings were governed by law);
- Number of data protection administrative proceedings *at the request of data subjects* 2018-2023: 1149 [Article 77 (1) of the GDPR];
- Number of data protection *ex officio* administrative proceedings 2018-2023: 197;
- Average percent per year of judicial review on the basis of the overall number of administrative proceedings (*ex officio and complaints*): 9,7%.






### 4.2. Questions about Corrective Supervisory Powers under the GDPR

Each Member States' supervisory authority is responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to data processing and to facilitate the free flow of personal data within the European Economic Area. In this regard, Article 57(1)(a) GDPR provides that each supervisory authority shall on its territory enforce the application of the GDPR.

This duty applies regardless of whether the supervisory authority acts *ex officio* or on the basis of a complaint.

However, in order to carry out this task the supervisory authorities must have effective toolsets, which allow them to take action against infringements of Regulation. For this reason, Article 58(2) GDPR provides for a set of corrective powers that a supervisory authority can use.

According to Article 58(2) of the GDPR each supervisory authority shall have all of the following corrective powers:

> (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
>
> (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
>
> (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
>
> (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
>
> (e) to order the controller to communicate a personal data breach to the data subject;
>
> (f) to impose a temporary or definitive limitation including a ban on processing;
>
> (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

*"Strong enforcement", "consistent and homogenous application of the rules", "equivalent powers for monitoring and ensuring compliance"*, *"equivalent sanctions for infringements"* and *"same tasks and effective powers, including (…) corrective powers"* are all called for by the recitals of the GDPR.[30] According the EDPB the consistent application of the corrective powers of the supervisory authorities is of key importance for the consistent level of protection in the European Economic Area.[31] This view is in accordance with that of data protection theory: *"[t]he GDPR this strengthens the system of the supervisory authorities and their independence and powers within a dedicated Chapter VI, and creates a mechanism for cooperation and consistency in Chapter VII."*[32]

However, the interpretation of the interplay of these supervisory powers raised questions especially with regard to the possible collision of the *ex officio* corrective powers of the Authority and the rights of the data subjects. This question was referred to the European Court of Justice to preliminary ruling by a Hungarian administrative court which can fundamentally determine the strength and the scope of the corrective powers of the data protection supervisory authorities in the future.

By its questions, the referring court asks, in essence, whether Article 58(2), in particular subparagraphs (c), (d) and (g), of the GDPR must be interpreted as meaning that the national supervisory authority, in exercise of its corrective powers, may order the data controller or processor to erase unlawfully processed personal data even in the absence of an express request by the data subject under Article 17(1) of the GDPR? In the event that the answer to the first question is that the supervisory authority may order the data controller or processor to erase unlawfully processed personal data even in the absence of a request by the data subject, is that so irrespective of whether or not the personal data were obtained from the data subject?

As regards the part of the decision ordering the erasure of personal data in the specific case, the applicant submits that Article 58(2)(d) of the GDPR does not give the Authority power to issue such an order. The applicant argues that the obligation on the data controller

[30] Recital 7, 10, 11 and 129 GDPR. See also Opinion 39/2021 on whether Article 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject (Adopted on 14 December 2021) See <edpb.europa.eu/system/files/2022-01/edpb_opinion_202139_article_582g_gdpr_en.pdf>.

[31] Opinion 39/2021 on whether Article 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject (Adopted on 14 December 2021) See <edpb.europa.eu/system/files/2022-01/edpb_opinion_202139_article_582g_gdpr_en.pdf>.

[32] Christopher KUNER-Lee A. BYGRAVE-Christopher DOCKSEY: The EU General Data Protection Regulation (GDPR) – A Commentary. Oxford University Press, Oxford, 2020. 942-943.

to erase data irrespective of whether the data subject has so requested flows from Article 5 of the GDPR rather than from Article 17(1) of that regulation, because the erasure under Article 17 of the GDPR can only be interpreted as a right of the data subject and the second part of the sentence in Article 17(1) can only be interpreted in the context of the exercise of that right, not independently but subject to the exercise of that right by the person concerned.

Before this request for preliminary ruling by decision No 3110 of 23 March 2022 the Hungarian Constitutional Court stated that, under Articles E (2) and (3) and VI (4) of the Hungarian Fundamental Law and in accordance with the GDPR — as EU legislation guaranteeing the uniform application of data protection and the freedom of information — the Authority has power to order *ex officio* the erasure of unlawfully processed personal data, including where there is no request by the data subject.

It seems that the Hungarian administrative court of first instance does not share fully the positions of the Constitutional Court. In this court's view, the right to erasure under Article 17 of the GDPR clearly must be interpreted as a right of the data subject and Article 17(1) does not establish two separate legal grounds for erasure. Instead, the second part of the sentence in that paragraph ('the controller shall have the obligation to erase [the data subject's] personal data without undue delay') is a subsequent obligation on the data controller deriving from the first part of that sentence. In consequence, contrary to the Board's Opinion 39/2021, this court is of the view that the right of erasure under Article 17 of the GDPR may only be interpreted as a right of the data subject. This is supported by the fact that the original text of the GDPR in English refers to the data controller's obligation using the conjunction 'and' between the first and second parts of the sentence in Article 17(1).

According to the court the question to be determined is, therefore, whether, irrespective of any exercise of his or her right by the data subject, the national supervisory authority may oblige the data controller or processor to erase the unlawfully processed personal data and, if it may, on what legal basis; in answering that question, it must be borne in mind, in particular, that Article 58(2)(c) of the GDPR is expressly predicated on a request to exercise the rights of the data subject and that Article 58(2)(d) provides in general terms that processing operations must be in compliance with the GDPR, while Article 58(2)(g) refers directly to Article 17 which, as explained above, likewise cannot be interpreted regardless of the need for an express request by the data subject to erase personal data.

For the Board to assess whether the power of the supervisory authorities under Article 58 (2)(g) of the GDPR applies even in the absence of a request for erasure from the data subject, it first had to consider whether Article 17 of the GDPR imposes an obligation on the controller only following a request from the data subject, or if this obligation is independent thereof. In this regard the Board found that Article 17 of the GDPR provides for two separate cases for erasure that are independent from each other: I. the erasure at the request of the data subject, and II. the erasure as a standalone obligation of the controller. This conclusion of the Board is supported by the fact that some cases set forth in Article 17(1) of the GDPR clearly refer to scenarios that the controllers must detect on their own as part of their obligation for compliance with the provisions GDPR, and by the rationale to allow supervisory authorities to ensure the enforcement of the principles enshrined in the GDPR even in cases where the data subjects are not informed or aware of the processing, or in cases where not all concerned data subjects have submitted a request for erasure. Based on the above reasoning, the EDPB concludes that Article 58(2)(g) of the GDPR is a valid legal basis for a

supervisory authority to order *ex officio* the erasure of unlawfully processed personal data in a situation where such request was not submitted by the data subject.[33]

The question can also be raised as to whether the data subject has the right to the illegality or whether the will (self-determination) of the data subject can set aside the whole GDPR even if the Authority found the processing totally unlawful. The judgment is expected in 2024.

### 4.3. Temporary Corrective Powers and the Online World

One of the biggest challenges is monitoring the online world and effectively intervening when necessary in "*data protection no-go zones*", especially on the dark web and several social media platforms. The Hungarian legislator - acting on the authority given by the GDPR[34] - therefore has given new powers to the Hungarian supervisory authority by modifying the Act CXII of 2011 and establishing the so-called "*blocking corrective powers"*: the order to remove and the order to render inaccessible electronic personal data.

As a first step and as a provisional measure to prevent the unlawful processing of personal data, the Authority may require also the hosting service provider or the intermediary service provider providing also hosting services on certain issues of electronic commerce services and information society services that processes the data published through an electronic communications network to temporarily remove the electronic data the publication of which serves as grounds for an authority proceeding for data protection or administrative audit by the Authority if in the absence thereof, the delay would cause an unavertable and severe violation of the right to personal data protection and

a) the data subject of the published data is a child, or

b) the published data is sensitive data or criminal personal data.

A procedural decision on the temporary removal of electronic data shall be communicated to the party subject to the removal obligation without delay. The party subject to the removal obligation shall be obliged to temporarily remove the electronic data within one working day from the communication of the procedural decision on the provisional measure by the Authority.[35]

Secondly as a provisional measure to prevent the unlawful processing of personal data, the Authority may order that the electronic data the publication of which serves as grounds for an authority proceeding for data protection or administrative audit by the Authority be rendered temporarily inaccessible. The electronic data may be rendered temporarily inaccessible where in the absence thereof, the delay would cause an unavertable and severe

[33] Opinion 39/2021 on whether Article 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject Adopted on 14 December 2021.

[34] Article 58(6) of the GDPR 6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII. See also*: "Article 58 is directly applicable. Hence, DPA's can rely on it directly when exercising their powers. However, Article 58 also leaves room for national legislation, both with regard to questions of procedural law and those of additional tasks."* KUNER- BYGRAVE-DOCKSEY (2020) 944.

[35] Section 61/A (1) -(2).

violation of the right to personal data protection, and any other measures, including temporary removal by the Authority under section 61/A (1) remained ineffective, and

a) the data subject of the published data is a child, or

b) the published data is sensitive data or criminal personal data.

The Authority shall communicate a procedural decision ordering the electronic data to be rendered temporarily inaccessible by public notice. The public notice shall be posted on the bulletin board and published on the website of the Authority for five days. The day of the communication of the procedural decision shall be the third day following the posting of the public notice. An obligation imposed by the procedural decision of the Authority shall apply to all electronic communications service providers without the need for an explicit provision to that effect.[36] The Authority may impose a procedural fine ranging from one hundred thousand forints (260 EUR) to twenty million forints (50.000 EUR) on an electronic communications service provider that fails to comply with its obligation set out in this section.[37]

### 4.4. Conflicts between the Authority and the Civil Courts

By introducing the administrative proceedings at the request of the data subject, it is not uncommon at all that data subjects lodge a complaint before the Authority and simultaneously an action before a civil court often with the same content, based on the same data protection provisions, asking the Authority (and thus the administrative court in case of judicial review) and the civil courts to interpret the same GDPR norm in the same case.

In this case Articles 77 to 79 of the GDPR almost necessarily give rise to a conflict between the administrative and judicial paths. The Court of Justice has interpreted Articles 77 and 79 of the GDPR from the point of view of the definition of the competences established in those provisions. The aforementioned articles confer on individuals rights enforceable in parallel, but the parallel exercise of those rights may give rise to uncertainty in relation to legal certainty, as is the case in the dispute of the case C-132/21. Since, in accordance with national procedural legislation, decisions of the Authority are not binding on the civil courts, it is not inconceivable that a civil court may adopt a decision contrary to that of the supervisory authority in relation to the same facts.

The role of an administrative court pursuant to the powers conferred by Article 78 of the GDPR is to review the decisions of the supervisory authority. The competences of the supervisory authority also define the competences of the administrative court, given that the latter may carry out an examination of lawfulness in respect of points of law falling within the scope of the supervisory authority's sphere of competence. The administrative court has an obligation to review the findings contained in the supervisory authority's decision on the infringement of the GDPR, the civil courts, acting pursuant to the powers provided for in Article 79 of that regulation, can give a final judgment on the same point of law. The judgment of the civil court lacks the authority of *res iudicata* in the dispute in the main proceedings because the parties to the proceedings are not identical. It can occur that the administrative court has to examine the same facts and the commission of the same infringement — and interpret the same EU and national legislation — as those/that in respect of which the civil court has already given final judgment. In accordance with national procedural law, even though the judgment of the civil court is not binding on the administrative court, [the latter

[36] Section 61/B (1) -(4).

[37] Section 61/B (6).

court] cannot disregard the general principle of legal certainty, whereby court decisions are binding on everyone (Article 6 of the Law on the organisation of the courts).

The parallel between competences at the vertical level is also problematic, given that the objective set out in recital 117 of the GDPR — according to which the establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data —, the achievement of which is an obligation incumbent on the Member States under Article 51(1), would be partially restricted if the legal action preceded the administrative appeal. In so far as it is permitted to bring the administrative appeal and the legal action in parallel, any final court order made first would be binding on the supervisory authority at the time of adjudicating on a complaint lodged on account of the same facts. In that situation, therefore, the competences of the supervisory authority as provided for in Article 58 of the GDPR would be restricted.

In case C-132/21 the Court finally ruled that Article 77(1), Article 78(1) and Article 79(1) of the GDPR read in the light of Article 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as permitting the remedies provided for in Article 77(1) and Article 78(1) of that regulation, on the one hand, and Article 9(1) thereof, on the other, to be exercised concurrently with and independently of each other. It is for the Member States, in accordance with the principle of procedural autonomy, to lay down detailed rules as regards the relationship between those remedies in order to ensure the effective protection of the rights guaranteed by that regulation and the consistent and homogeneous application of its provisions, as well as the right to an effective remedy before a court or tribunal as referred to in Article 47 of the Charter of Fundamental Rights.

Since the Hungarian legislation does not contain any regulations regarding parallel legal remedies, the issue is not closed yet. The Authority respects the judgments of the civil courts even if, as this was the case in C-132/21, the legal position of the civil judge is contrary to the Authority's interpretation. The referring court was right though by stating that this situation resulting from the GDPR, may lead to the infringement of one of the most important EU principle: the rule of law. Numbers show in Hungary that the number of civil remedies is negligible compared to the administrative ones. No wonder, since the Authority has much stronger powers, its administrative proceeding is free from red tape, on the other hand civil court procedures are claimed to be excessive and rigid and the compensations for (reputation) damages are relatively low.

## 5. Conclusions

GDPR has proved to be a game changer. It has brought revolutionary changes, the fundamental and complete transformation of the role of supervisory authorities, its proceedings and relationship with the judiciary. GDPR has radically raised privacy-awareness across organisations of any kind and it is a radical breakthrough in data subjects', data controllers' and the courts' (!) beliefs and behaviours with regard to the importance of data protection.

Over the past 30 years, Hungarian data protection law has come a long way, with a number of substantive, procedural and organisational changes. Nevertheless, the tendencies are clearly moving in one direction: due to the brutal growth of the digital age and the data-based economy and services, the exercise of the right to the protection of personal data

requires strong and effective powers. The development of data protection law in Hungary has already directed the organisational and procedural legal framework to an administrative-type model by establishing a more and more effective toolbox of corrective powers before the GDPR and in some sense even before the Act CXII of 2011.

As regards the role of administrative justice in this process, the initial passive, rather abstaining attitude has been overturned by the above process, and the Hungarian administrative judiciary increasingly and more and more actively claims a decisive role in interpretation of data protection law.

However, this process is far from over, on the contrary we are at the very beginning. The case- law of the Court is still evolving and important questions of substantive and procedural law remain to be answered.

Paraphrasing József Attila's famous lines, based on historical experience there'll be always enough reason to look up the file which violates someone's rights. The real question is whether data protection legislation remains a dead letter or by means of legally and practically enforceable supervisory powers, the principles and rules protecting our privacy come to life.

**Bibliography:**

1. Act LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices (Competition Act).
2. Data Protection Commissioner's 2008 Report, 134-135.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) OJ 2016 L 119, p. 1 / GDPR.
4. The Fundamental Law of Hungary (25 April 2011).
5. *Kuner C., Bygrave L.A., Docksey C.,* The EU General Data Protection Regulation (GDPR) – a Commentary, Oxford University Press, Oxford, 2020, 942-943.
6. Opinion 39/2021 on whether Article 58(2.g), Adopted on 14 December 2021.
7. Kúria Kf.VI.37.956/2018/6.
8. Kúria Kfv.III.37.911/2017/8.
9. Budapest Court of Hungary K.33.024/2004/46.
10. Judgment of 1 October 2015, Weltimmo, C-230/14, EU:C:2015:639
11. Report of 2005 of the Data Protection Commissioner, 45-46;
12. Supreme Court of Justice of Hungary Kfv.37.923/2010/5.
13. Supreme Court of Justice of Hungary Kfv.V.35.180/2009/5.
14. Vas County Court of Hungary 1.K.20.018/2009/33.